Clifton Gunderson LLP
Certified Public Accountants & Consultants

Independent Auditor's Report

To the Inspector General
Library of Congress

We have audited the accompanying consolidated balance sheets of the Library of Congress (Library) as of September 30, 2000 and 1999, and the related consolidated statements of net cost, changes in net position, and combined statements of budgetary resources for the years then ended (collectively the Financial Statements). These Financial Statements are the responsibility of the Library's management. Our responsibility is to express an opinion on these Financial Statements based on our audits.

We conducted our audits in accordance with U. S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.* These standards and requirements require that we plan and perform the audit to obtain reasonable assurance about whether the Financial Statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the Financial Statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the Financial Statements including the accompanying notes present fairly, in all material respects, the financial position of the Library of Congress as of September 30, 2000 and 1999, and its net costs, changes in net position, and budgetary resources for the years then ended, in conformity with U. S. generally accepted accounting principles.

In accordance with *Government Auditing Standards*, we have also issued our reports dated March 2, 2001 on our consideration of the Library's internal control over financial reporting, and our tests of its compliance with certain provisions of laws and regulations. These reports are an integral part of our audits performed in accordance with *Government Auditing Standards* and should be read in conjunction with this report in considering the results of our audits.

Centerpark I
4041 Powder Mill Road, Suite 410
Calverton, Maryland 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

Our audits were made for the purpose of forming an opinion on the basic Financial Statements taken as a whole. The information contained in Management's Discussion and Analysis, the supplemental consolidating information, and the Required Supplementary Stewardship information is not a required part of the basic Financial Statements but is supplemental information required by OMB Bulletin No. 97-01, *Form and Content of Agency Financial Statements.* This information contains a wide range of data, some of which is not directly related to the Financial Statements. We have applied certain limited procedures, which consisted principally of comparing this information for consistency with the Financial Statements and discussing the methods of measurement and presentation with Library officials. Such information has not been subjected to the auditing procedures applied in the audits of the basic Financial Statements, and, accordingly, we express no opinion on it.

Clifton Gunderson LLP

Calverton, Maryland
March 2, 2001

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Independent Auditor's Report On Compliance With Laws and Regulations

To the Inspector General
The Library of Congress

We have audited the Financial Statements of the Library of Congress (Library) as of and for the years ended September 30, 2000 and 1999, and have issued our report thereon dated March 2, 2001. We conducted our audits in accordance with U. S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.*

The management of the Library is responsible for complying with laws and regulations applicable to the Library. As part of obtaining reasonable assurance about whether the Library's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and certain other laws and regulations specified in OMB Bulletin No. 01-02. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to the Library.

The results of our tests of compliance with the laws and regulations described in the preceding paragraph disclosed the following instances of noncompliance with certain laws and regulations that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 01-02.

- During fiscal years 2000 and 1999 the Library operated ten revolving gift funds beyond the scope of its authority. The Library has transmitted draft legislation to the appropriate authorizing committees on a yearly basis since 1991 to address this issue. An amended version of the Library's revolving fund legislation was enacted into law when the "Library of Congress Fiscal Operations Improvement Act of 2000" was approved in November 2000. The Act will be effective at the start of fiscal year 2002 and the Library will then be in compliance.

Centerpark I
4041 Powder Mill Road, Suite 410
Calverton, Maryland 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

- During fiscal years 2000 and 1999, the Library was not in compliance with the "Congressional Accountability Act (CAA) of 1995." In the CAA, Congress made its facilities and employees subject to the same safety laws that applied outside the legislative branch. In 1997, other provisions of the CAA applied fire safety standards to Congressional buildings, including the Library. The Office of Compliance conducted a yearlong fire safety investigation that culminated in a report issued in January 2001 that identified numerous safety hazards in the Library's three Capitol Hill buildings.

The results of our tests of compliance disclosed no instances of noncompliance with other laws and regulations discussed in the preceding paragraph that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 01-02.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit and, accordingly, we do not express such an opinion.

This report is intended solely for the information and use of the Library, the Library's Office of the Inspector General and Congress, and is not intended to be and should not be used by anyone other than these specified parties. We caution that non-compliance may occur and not be detected by the tests performed and that such testing may not be sufficient for other purposes.

Clifton Gunderson LLP

Calverton, Maryland
March 2, 2001

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Independent Auditor's Report On Internal Control

To the Inspector General
The Library of Congress

We have audited the Financial Statements of the Library of Congress (Library) as of and for the years ended September 30, 2000 and 1999 and have issued our report thereon dated March 2, 2001. We conducted our audits in accordance with U. S. generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and, Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.*

In planning and performing our audits, we considered the Library's internal control over financial reporting (excluding safeguarding collection assets) by obtaining an understanding of the Library's internal control, determined whether internal controls had been placed in operation, assessed control risk, and performed tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 01-02. As the Library is not subject to the requirements of the Federal Managers' Financial Integrity Act (31 U.S.C. 3512) (FMFIA), we did not test internal controls relevant to operating objectives as broadly defined by FMFIA, such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal control. Consequently, we do not provide an opinion on internal control. We issued our report dated March 2, 2001 on management's assertion about the effectiveness of internal controls over safeguarding collection assets.

Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control over financial reporting that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of the internal control that, in our judgment, could adversely affect the Library's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that

misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. However, we noted certain matters discussed in the following paragraphs involving the internal control and its operation that we consider to be reportable conditions.

In addition, we considered the Library's internal control over Required Supplementary Stewardship Information by obtaining an understanding of the Library's internal control, determined whether these internal controls had been placed in operation, assessed control risk, and performed tests of controls as required by OMB Bulletin No. 01-02, and not to provide assurance on these internal controls. Accordingly, we do not provide assurance on such controls.

As the Library is not subject to the requirements of the Government Performance and Results Act (GPRA), and the performance measures reported in the Management's Discussion and Analysis are not related to implementation of the GPRA, we did not obtain an understanding of the design of internal controls relating to the existence and completeness assertions of such measures.

****

REPORTABLE CONDITIONS

1. SECURITY PRACTICES OVER INFORMATION TECHNOLOGY SYSTEMS NEED TO BE IMPROVED

Our audit found that the Library's systems environment remained threatened by weaknesses in several information protection control structures. The controls in place were inadequate to fully protect information systems' resources from unauthorized access, unauthorized use, or damage. The Library had not implemented security policies and procedures to ensure that Library resources were restricted to authorized individuals and that critical data was protected. The presence of these weaknesses increases the risk that the Library's data and equipment are not properly safeguarded. The details of the matters are as follows:

- ***Entity-Wide Security Program is inadequate.*** The Library lacks a comprehensive security administrative structure to manage and protects its diverse and varied information technologies. The Library has only one security officer to manage and monitor all of its information technologies. The Library's current management procedures and organizational framework are deficient for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the

effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems on an ad hoc basis, or after a violation has been detected or an audit finding has been reported.

- ***The Library's logical access controls do not sufficiently restrict access.*** Logical access controls were inadequate to ensure the safekeeping of sensitive utilities and data sets. A number of logical access controls settings were not in place. The Library lacks the administrative structure and management policies to manage access controls for applications and system software. There are no written standard access control policies. During our review of system programmers access privileges, we found one system programmer's ID is still active after leaving the Library's employment over a year ago. The ID has the highest of access privileges. The security package that protects the financial application is obsolete and is not supported by the vendor. The special privileges attributes in the security software are not implemented to enhance security. We also discovered that members of System Engineering Group (SEG) can bypass the security software and can access the sensitive information in the Federal Financial System (FFS) without an audit trail.

- ***Application security controls should be strengthened.*** Application controls do not include a program for the certification and accreditation of sensitive applications. Management control over computer security was impaired by the lack of a process for the technical evaluation of the security of sensitive applications. Not addressing these control weaknesses increases the risk of unauthorized access to certain sensitive applications and data without being detected.

- ***Application software, system software, and change controls were inadequate.*** The Library does not have controls in place for the management and maintenance of application and systems software. There were no written standards to control production programs as they progress through testing to final approval. The lack of controls may result in inefficient or inadequate testing or introducing production programs that do not meet management's criteria. The Library does not maintain adequate controls of the its test and production libraries. We found that the Financial Services Directorate submitted programs that updated the Federal Financial System (FFS) from a library other than the production library.

Recommendation:

We recommend the following:

- We recommend that the Library implement security policies and procedures to ensure that Library resources are restricted to authorized individuals and that critical data is protected. Also, we recommend that senior management make security of its information systems a higher priority and allocate adequate resources and personnel. We recommend that senior management establish a structure to implement the security program throughout the entity. The structure generally consists of a core of personnel who are designated as security managers. These personnel play a key role in developing, communicating, and monitoring compliance with security policies and reporting on these activities to senior management. The security management function also serves as a focal point for others who play a role in evaluating the appropriateness and effectiveness of computer-related controls on a day-to-day basis. These include program managers who rely on the entity's computer systems, system administrators, and system users.

- Develop administrative structures and management policies to manage access controls and develop a standard access control policies for main frame as well as client-server systems and applications. In addition, deactivate the access privilege of users ID's who have left the Library's employment;

- Develop and implement controls to ensure that the configuration of sensitive utilities and security software are set to minimize exposure to unauthorized access and un-logged activities. Perform risk assessments to determine the need for group access and compensating controls that minimize the risk exposure;

- Evaluate and review the implementation of security features available in the operating systems and applications to ensure that risks, security and compensating controls have been addressed and to upgrade the security package to protect the financial application;

- Establish a program for the certification and accreditation of major application systems and general support systems in accordance with the Federal Information Processing Standards Publication (FIPS PUB) 102 "Guideline for Computer Security Certification and Accreditation"; and

- Develop a written Systems Development Life Cycle methodology. Also, develop and implement controls for emergency system software changes and prohibit users from submitting test programs that update production data.

2. THE LIBRARY LACKS A BUSINESS CONTINUITY PLAN

The Library does not have a service continuity plan. The Library does not have critical policies and procedures usually found in government and private industry to protect information resources and minimize the risk of unplanned interruptions and to recover critical operations should interruptions occur. There is no management or administrative structure to implement or maintain service continuity of the Library operations. Also, the Library does not have standard written policies for performing backups of data files, computer programs, and critical documents and placing them in off-site storage.

The Library could lose the capability to process, retrieve, and protect information maintained electronically in the event of a disaster. Such an event would have a significant impact on its ability to accomplish its mission.

Recommendation:

We recommend that the Library:

- Develop management policies and administrative structure to implement or maintain services continuity of the Library operations, and develop standard backup written policies for performing backups of data files, computer programs, and critical documents and placing them in off-site storage,

- Assess the criticality and sensitivity of computerized operations and identify supporting resources,

- Train staff to respond to emergencies,

- Develop policies that prohibit eating and allowing liquids in data center, and

- Monitor hardware maintenance of environmental controls in the data center.

We also recommend that the Library immediately develop and test a disaster recovery plan for its data center and other information technology facilities.

****

Relevant comments from the Library's management responsible for addressing these internal control matters are provided as an attachment later in this section.

In addition to the reportable conditions described above, we noted certain matters involving internal control and its operations that we reported to the management of the Library in a separate letter dated March 2, 2001.

This report is intended solely for the information and use of the Library, the Library's Office of the Inspector General and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Gunderson LLP

Calverton, Maryland
March 2, 2001

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Independent Auditor's Report On Management's Assertion About The Effectiveness Of Internal Controls Over Safeguarding Collection Assets

To the Inspector General
The Library of Congress

We have examined management's assertion, which is presented in Section 4, that it cannot provide reasonable assurance that the Library of Congress' internal control structure over safeguarding of collection assets against unauthorized acquisition, use, or disposition was generally effective as of September 30, 2000.

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants and with *Government Auditing Standards*, issued by the Comptroller General of the United States, and accordingly included obtaining an understanding of the internal control structure over safeguarding of collection assets, testing and evaluating the design and operating effectiveness of the internal control structure, and such other procedures as we considered necessary in the circumstances. We believe our examination provides a reasonable basis for our opinion.

Because of inherent limitations in internal controls, unauthorized acquisitions, use, or disposition of collection assets may occur and not be detected. Also, projections of any evaluation of internal controls over safeguarding of assets to future periods are subject to the risk that internal controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In its assertion letter, the Library of Congress had defined the following control criteria for safeguarding collection assets against unauthorized acquisitions, use or disposition:

- **Bibliographic controls**, which include but are not limited to: cataloging, archival processing, and arrearage reduction;

- **Inventory controls**, which include but are not limited to: item-level holdings records and bar-coding for non-rare monographs accessioned October 1999 or later; the automated circulation control system as implemented in the Integrated Library System (LC ILS); manual and automated shelf list and serial records; finding aids and other detailed item and/or collections descriptions, and registry of items lent for exhibition.

Centerpark I
4041 Powder Mill Road, Suite 410
Calverton, Maryland 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

- **Preservation controls**, which include but are not limited to: use of surrogates (digital, microform, service copies of audiovisual materials); collections care programs; disaster preparedness; Top Treasures security; de-acidification; conservation of individual items; preservation treatment of processed items, preservation research and testing programs to define actions for de-acidification, storage, audio preservation;, studies of longevity of new digital media, etc.; and special Congressionally-mandated preservation programs such as the National Film Preservation Board and American Television and Radio Archive.

- **Physical security controls**, which include but are not limited to: perimeter security (e.g., theft detection devices); secured receiving and holding areas for materials not yet accessioned into the research collections, including the Copyright Office; secured in-process working and holding areas; storage areas closed to the public and all staff except those who require daily access in order to perform their jobs; reader registration; security in reading rooms (cameras, police and guard patrols, etc.); caging of high risk collections; and secured loan stations.

The Library asserted that specific controls over items in the collection assets depend upon the individual format, demand for and condition of use, and the value and risk assessment for that item. The *Integrated Control-Integrated Framework,* issued by the Committee of Sponsoring Organizations of the Treadway Commission, would classify the aforementioned Library criteria as "control activities." The Integrated Framework also includes the following elements of internal control reporting:

- Risk assessment and collections security plan – The Library must assess the risk of unauthorized acquisition, use, or disposition of the collection;

- Control environment – The Library must influence the control consciousness of its personnel by instituting an environment that makes internal control a priority;

- Information and communication – The Library must determine what information is needed by management to prevent or timely detect control failures and make that information readily available to management at all times; and

- Monitoring – The Library must establish policies and procedures for monitoring compliance with internal controls by personnel assigned to those tasks.

Adapting these elements to the *Internal Control-Integrated Framework's* definition of internal controls over safeguarding of assets to fit the Library's circumstances can be summarized as follows:

"Internal control over the safeguarding of collections against unauthorized acquisition, use, or disposition is a process, effected by the Library's management and other personnel, designed to provide reasonable assurance that the risk of unanticipated loss (theft, mutilation, destruction, or misplacement) of collection items of significant market value, cultural or historical importance, or significant information value is reduced to an acceptable level."

Applying this definition using the Library's control criteria, a weakness in safeguarding controls is significant enough that it should be included in the Library's assertion if it results in either:

- Significant risk of unanticipated loss (theft, mutilation, destruction, or misplacement) of collection items of significant market value, cultural or historical importance, or significant information value, or

- Significant risk that senior Library management does not have sufficient information about the extent to which the Library's objectives concerning the safeguarding of the collections are being achieved.

The Library has identified such weaknesses as material weaknesses based on guidance provided by the General Accounting Office.

Opinion on Management's Assertion

The Library aggressively addressed deficiencies in bibliographic, inventory, preservation, and security controls in the past fiscal year, however in its assertion, management identified material weaknesses summarized below which could adversely affect the Library's ability to meet its internal control objectives. As a result, the Library cannot provide reasonable assurance that the internal control structure over safeguarding the Heritage Assets against unauthorized acquisition, use, or disposition was completely effective as of September 30, 2000 for all of the Library's collections.

With the implementation of the LC ILS and the application of bar codes to all newly accessioned non-rare monographs beginning October 1999, the Library has taken a step towards partitioning its assertion. The Library cannot assert without qualification that the controls in place are adequate and appropriate to mitigate the risks for all the special collections, but the Library does assert that newly-acquired non-rare monographs (a major portion of the general collections of the Library) are under bibliographic, inventory (when it is circulated outside the Library), preservation and physical security controls.

In its assertion, management describes significant weaknesses in preservation controls, inventory controls, bibliographic controls, and physical security controls over collection assets as of September 30, 2000. Our recommendations for certain of these and other significant weaknesses identified by us during our examination are outlined in the following section, *Internal Control Weaknesses in Safeguarding of Collection Assets and Recommendations for Improvement*. Our current year recommendations and assessment of the Library's initiative are intended to build on the findings and recommendations made in prior years.

In our opinion, management's assertion that, as a result of the material weaknesses in controls described in its report, it cannot provide reasonable assurance that the internal control structure over safeguarding collection assets against unauthorized acquisition, use, or disposition, was generally effective as of September 30, 2000, is fairly stated based upon the criteria described above. In addition, management's assertion that, newly-acquired non-rare monographs (a major portion of the general collections of the Library) are under generally effective bibliographic, inventory (when it is circulated outside the Library), preservation and physical security controls as of September 30, 2000, is fairly stated based upon the criteria described above.

This report is intended solely for the information and use of the Library, the Library's Office of the Inspector General and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Gunderson LLP

Calverton, Maryland
March 2, 2001

INTERNAL CONTROL WEAKNESSES IN SAFEGUARDING OF COLLECTION ASSETS AND RECOMMENDATIONS FOR IMPROVEMENT

1. A WEAK CONTROL ENVIRONMENT AND INCOMPLETE CONTROL ACTIVITIES EXISTED FOR THE SAFEGUARDING OF THE COLLECTION ASSETS

The Library of Congress, as the nation's library of last resort, has a special obligation to acquire comprehensively the creative and intellectual legacy of this nation; to secure and preserve those items for present and future generations; and to make these items as available as possible and prudent to its constituents, primarily the Congress, other branches of government, and the research community. Achieving and maintaining the proper balance among preservation, security, and access is a dynamic and challenging process, faced by all libraries and archives. The Library is custodian of nearly 121 million items, in over 450 languages and in many formats, including but not limited to: manuscripts, maps and globes, motion pictures, rare books, and digital files.

In its assertion, management describes a number of significant weaknesses in bibliographic controls, inventory controls, preservation controls, and physical security controls over collections as of September 30, 2000. Management also describes initiatives the Library has undertaken since September 30, 1997 to remedy some of these weaknesses.

Bibliographical controls: During fiscal year 2000, newly acquired items were accessioned and cataloged using the LC ILS. The Library continued to reduce the arrearage count: at September 30, 2000 19.2 million items were in arrearage, reduced from the 1989 benchmark number of 39.7 million items.

Inventory controls: Contracts were let and work begun on the conversion of the 12 million card shelflist of printed books and the conversion of the serials check-in file and holdings files. The conversion of both of these enormous files is a requisite step before a physical inventory can be commenced.

Preservation controls: The Library had inadequate temperature and humidity control in some collections storage areas; inadequate for appropriate storage of collections materials; insufficient space for reformatting the acetate negative collection; and insufficient funds for reformatting.

Physical security controls: In fiscal year 2000, the Library integrated its preservation, bibliographic, and inventory controls within the security planning framework developed for the 1997 security plan. An additional life-cycle element was added to the security plan to govern collections items on exhibit. The Library continued implementation of actions outlined in the 1997 security plan including, opening a larger reader registration facility in the James Madison Building; contracting for additional security monitors in reading rooms, and tagging and marking library materials in the retrospective collections.

Recommendations:

We recommend the Library continue to take action on improving the control environment and implementing control activities, based on the 1997 security plan. We recommend the Library to continue to revise the 1997 security plan as conditions change and improvements are identified. We support the Library's request for an inventory of the general collections, a project that would take several years. That project, the process of comparing the book stock on the shelves to inventory records that are currently being converted to digital format, would establish a benchmark from which future security assessments could be measured.

2. THE LIBRARY COLLECTION SECURITY PLAN HAS NOT BEEN FULLY IMPLEMENTED

The Library's Security plan was not fully implemented. Although the Library continued to implement actions outlined in the 1997 security plan, the Library has not established control activities to mitigate identified risks to the collection and has not completed establishment of the policies and procedures necessary to implement the necessary controls. The Library has not yet implemented a system for providing the required management information needed for management to carry out its responsibilities, nor has it established the methods by which management will monitor the effectiveness of the established control procedures.

Measurements of the effectiveness of the Library's physical security controls hinge on the development of credible baselines. Conducting regular inventories and/or statistically valid random sampling efforts can create baselines capable of establishing trends in theft and mutilation.

The Library has taken a number of initiatives in fiscal years 1999 and 2000 to address prior findings related to collections security.

Recommendations:

We recommend that the Library take action to fully develop and implement its security plan. The Library's security plan focuses on physical security and procedural standards and requirements for protecting the collections. We recommend that the Library take the necessary actions to fully develop and implement the programs that are essential to the full implementation of the security plan.

We also recommend that the Library continue conducting regular inventories and/or statistically valid random sampling projects in select divisions. These measuring projects will create valid baselines, which over time will yield trends in theft and mutilation enabling Library's management to evaluate the effectiveness of its Security Plan and controls in place protecting the collections.

3. THE LIBRARY LACKED EFFECTIVE MANAGEMENT INFORMATION FOR MONITORING OF THE COLLECTIONS ASSETS' INTERNAL CONTROLS

Collection security objectives were incorporated in annual performance plans of custodial chiefs in fiscal year 1999. Meaningful and regular management information about whether security goals are being established and met is essential to a strong control environment. The performance plans of security officials and custodial division chiefs, as well as those in other service units who are responsible for collections security, should include measurable objectives for assuring all collections controls are implemented and functioning. Now that the risk assessments are performed, it is known what tasks personnel should perform. Action plans were prepared, by the management in each division, in response to the Risk Assessments.

Recommendations:

We recommend monitoring the integration of the performance plan process with the Library's collection risk assessments. The major controls over safeguarding of collection assets have been identified from the risk assessments. Each division has developed measurable tasks that personnel should be performing to assure that those controls are functioning. Division management should be held accountable for monitoring personnel assigned to these tasks. Reporting these results should be fully integrated into the Library's annual performance plans in order that management receives the information needed to assess the effectiveness of the internal controls over the collection assets.